Criminal Investigation Management Information System (CIMIS) – Privacy Impact Assessment (PIA)

PIA Approval Date: July 1, 2009

System Overview

The Criminal Investigation (IRS CI) Management Information System (CIMIS) is a management and information system for tracking the status and progress of CI investigations, time expended by CI employees, employee information, and IRS CI investigative Equipment. The management reports in this system provide special reporting capabilities required for enforcement activities, e.g., tracking arrests, indictments, search warrants and seizures. CIMIS' objective is to provide the vehicle to collect, compile, and deliver accurate real time information to all levels of Criminal Investigation management and internal/external stakeholders. The CIMIS application will integrate with a new application named AFTRAK. When released, the CIMIS R2.5 system will be comprised of both CIMIS and AFTRAK applications.

Systems of Records Notice (SORN):

- Treasury/IRS 46.002 – CIMIS
- Treasury/IRS 34.037 – IRS audit trail and security records system

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

CIMIS

A. Taxpayer – Includes data related to the identity of the individual, the tax forms they have filed, an estimated criminal tax deficiency, terms of probation involving taxes, and other information regarding potential criminal tax and other financial investigations.

- Name
- Doing Business As (DBA)
- Alias
- Identity Type
- Affiliation to Subject
- Taxpayer Information Number (TIN)
- Other Identifying Numbers (driver's license, passport, etc.)
- Address
- Date of Birth
- Gender
- Type of Tax Forms
- Preparer Name

B1. CI Employee – Compared to investigative data, employee data is stored in separate business tables, tracked in separate log tables, and access granted based on separate user roles.

- Name
- SSN (in future updates to CIMIS, employee SSNs will be partially or completely masked in the majority of the screens and reports, with the ultimate goal being the

elimination of employee SSNs from the CIMIS database altogether)

- Identification Number (SEID)
- Date of Birth
- Retirement Plan and 6C Date
- Service Computation Date
- Award/Type
- Type/Date of Background Investigation
- Security Clearance
- Skills
- Education/Degree/Graduation
- Position
- Management Assignments and Training
- Time Reporting Data

B2. Non-CI Employee – Non-CI employee data is limited to name, title and organization within specific investigative data, e.g., a requesting or cooperating revenue agent. The employee can be another IRS employee.

- Name
- Address
- Phone Information
- CI Affiliation

C. Audit Trail

- Date/Time Stamp (The Date/Time of when the audit record was created),
- Unique Identifier (The Unique Identifier that initiates the action for the audit record, such as the user name or SID),
- Event Type (The Event Type field is used to track the type of event that is executed such as add, update, or delete),
- Origin of Request (The origin of where the request was made, such as the Terminal ID),
- Name of Object (The name of the object that was introduced, accessed, or deleted),
- User Identity (The identity of the user who performed the action),
- User Role (The role of the user at the time the action was performed)

D. Other – Inventory and assignment of equipment and vehicle expense and mileage information. Strictly speaking, the below data does not contain privacy information; however, equipment inventory is tied to an employee within CIMIS, and as a result could be used to ultimately identify an individual.

- Equipment ID Number
- Order Information (date, intended organization, etc.)
- Acquisition Information (date, amount, etc.)
- Category/Sub-category/Sub-category Class
- Description
- Purpose
- Manufacturer
- Model
- Serial Number
- Vehicle Specific Information (model year, license plate #, initial odometer reading, etc.)
- Vehicle Maintenance Expenses and Mileage Information

- Shipment and Consignment Information
- Assignment and Storage Information
- Disposal Information (dates, disposal, proceeds)

<u>AFTRAK</u>

A. Taxpayer

- Name
- Doing Business As (DBA)
- Alias
- Address

B. Employee

- Seizing Agent First and Last name (this information is retrievable from CIMIS but never stored as data elements in AFTRAK)
- Asset Forfeiture Coordinators First and Last Name, Phone Number, and Address

C. Audit Trail

- Date/Time Stamp (The Date/Time of when the audit record was created),
- Unique Identifier (The Unique Identifier that initiates the action for the audit record, such as the user name or SID),
- Event Type (The Event Type field is used to track the type of event that is executed such as add, update, or delete),
- Origin of Request (The origin of where the request was made, such as the Terminal ID),
- Name of Object (The name of the object that was introduced, accessed, or deleted),
- User Identity (The identity of the user who performed the action),
- User Role (The role of the user at the time the action was performed)

D. Other

- Information on individuals who have been identified as having an interest in an asset (such as an owner, lien, claim, or petition). This information includes: Name, Address, Phone Numbers, Aliases, Email Address, Attorney Name, Attorney Phone, Attorney Fax, and Attorney Email Address.
- Contact Names of agents from other agencies (federal, state, or local) that have requested a share in the proceeds of an asset that their agency helped IRS seize and forfeit.
- Names and addresses of Storage Location Vendors.
- Asset description may contain identifying information, to include bank account numbers and vehicle identification numbers. This depends on the type of asset seized.
- Vehicle Identification Numbers, Serial Numbers, License Plate Numbers, and Account Numbers are also stored

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

<u>CIMIS</u>

A. IRS – IDRS (identity and tax return information - see 1.A above) – this data is manually entered into CIMIS.

B. Taxpayer – Identity and tax return information may be provided by the taxpayer or their designated representatives through interviews and document requests (identity and tax return information, see 1.A above)

C. Employee – (all employee related information, see 1.B above)

D. Other Federal Agencies – Agency investigative data is generally not reflected in CIMIS; however, some exceptions include:

- The Department of Justice (DOJ) may provide administrative information (legal opinions/authorizations) and results of judicial proceedings that are reflected in CIMIS as status and/or arrest/fugitive updates.
- Financial Crimes Enforcement Network (FinCEN) may provide taxpayer identity information (see 1.A above)
- United States Postal Inspection Service (USPIS) may supply mail cover approvals and corresponding dates
- Any agency may provide or confirm identity information and criminal allegations

E. State and Local Agencies – Agency investigative data is generally not reflected in CIMIS. Any agency may provide or confirm identity information and criminal allegations. (Taxpayer identity information, see 1.A above.)

F. Other third party sources – Informants and other third party source information is generally not reflected in CIMIS. Their names may be listed as associate identities or they may provide additional taxpayer identifying information and criminal allegations. (Taxpayer identity information, see 1.A above). Time reporting data may be uploaded from the Diary application which is part of the CI Standard Applications package residing on the agents' personal workstations.

<u>AFTRAK</u>

A. IRS – The CIMIS Number is fully integrated with the AFTRAK system. The application pulls in data from the application to reduce redundancy of data.

B. Taxpayer – none

C. Employee – (all employee related information, see 1.B above)

D. Other Federal Agencies – TEOAF provides National Finance Center (NFC) data that is matched with data in AFTRAK. Users view reports showing matched and unmatched data in order to reconcile differences. This information contains no privacy information, and is only an asset number and an amount. In addition, AFTRAK stores data received from DOJ that contains information concerning Reverse Asset Sharing Requests (RASR).

U.S. Customs Seizure Case and Asset Tracking System (SEACATS) data is provided to AFTRAK via Contract Asset Property Managers. The SEACATS data is matched with data in AFTRAK. Users view reports showing matched and unmatched data in order to reconcile differences. This information contains vendor name and address.

E. State and Local Agencies – None

F. Third Party Resources – A Contract Asset Property Manager provides US Customs SEACATS data.

3. Is each data item required for the business purpose of the system? Explain.

CIMIS

Yes. The data collected is required for CIMIS to track CI investigations, employee data, hours spent on investigations, and equipment inventory.

AFTRAK

Yes. Assets must be stored and maintained by the government until asset disposition decisions are made. AFTRAK is the inventory tool for these assets which supports the business purpose of the system.

4. How will each data item be verified for accuracy, timeliness, and completeness?

CIMIS

Different levels of CI Management will be responsible for reviewing data entries in CIMIS. Periodic reviews and inventories are conducted specifically to measure the accuracy, timeliness and completeness of data entered into CIMIS. In addition, CI Management conducts complete reviews of the inventory within CIMIS once every three years to ensure accuracy. CIMIS does not receive data from other systems. However, for data entered into the system, validity checks within the application are utilized to verify accuracy and completeness.

AFTRAK

The Asset Forfeiture Specialist employee category of users is made up of contractors responsible for entry of the data which is then validated by the Asset Forfeiture Coordinator employee category, which are IRS employees. The business rules built into the application ensure that accuracy and completeness of the data entered.

Manual imports of extracts from the following external entities are received: The TEOAF, National Seized Property Contractors (NSPC), and the DOJ. The data that is imported is reconciled against the data that is input through the AFTRAK user interface for accuracy. The imports themselves are used as a mechanism to verify that the data in AFTRAK is accurate.

5. Is there another source for the data? Explain how that source is or is not used.

CIMIS

Yes. Employee time records can be accessed via Diary. Diary is a desktop application used by agents to record their time. While CIMIS is the source of record, data is stored semi-permanently in that desktop application until it is recorded into CIMIS. However, there is no other source of data for the type of information that will be contained in CIMIS.

AFTRAK

No. There are no other sources of data beyond what has already been mentioned previously in this PIA.

6. Generally, how will data be retrieved by the user?

CIMIS

Data will be retrieved either through the view and edit capability of the application, from preformatted reports, and/or a designed query.

AFTRAK

AFTRAK application users can use the Investigation Number, Seizure Number and AFTRAK Number to retrieve data. The investigation number is directly related to the CIMIS investigation. The seizure number is only an identifying number for AFTRAK and not privacy related data. The AFTRAK Number is a unique identifier for the specific assets related to a seizure and does not contain privacy related data.

AFTRAK Report users retrieve data based on the data scope. Data scope is either National (all data), region (data for all field offices in region, or field office (only data within their field office).

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?

CIMIS

Yes. Employee data can be retrieved by name, SSN, SEID, and a system generated unique identifier. Mitigation will be implemented wherein employee data is only retrievable by SSN by HQ staff charged with data administration. End users will no longer be able to retrieve employee records by searching on SSN.

CI Employee data must be maintained per Internal Revenue Manual (IRM) 1.15.30 Records Management, Records Control Schedule for Criminal Investigation, January 1, 2003. Prior to SEID number being assigned to IRS CI employees only the SSN was used to provide information on CI employees. The SSN is the only valid number to identify former employees and employees whose marital status has changed, i.e., last name. Investigation data can be retrieved by name, TIN and system generated unique identifier. Equipment data can be retrieved by assignment name and a system generated unique identifier.

AFTRAK

Yes. Employee data may be retrievable by first name or last name. AFTRAK does not store SSN or TIN.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

CIMIS

All CI personnel (Users, Managers, System Administrators, Developers, Others) can gain access to the system if approved by Management. Access controls are in place and are enforced primarily by controlling access to the Windows based operating system and by controlling access to CIMIS itself through the use of user roles that grant activity permissions and limit the organizational data scope for those permissions to five main areas: Personnel, equipment, administrative, investigation, and time reporting. Individuals are given read write or approval roles to the data contained within a given area. In addition, each section has a super user role that allows the user to correct and fix data within that section.

For a complete listing of user roles and their permissions, please see the Roles and Activities Matrix. This matrix is too large to include in this document, but can be obtained by contacting the “Requesting Contact” named at the beginning of this document.

AFTRAK

All CI personnel (Users, Managers, System Administrators, Developers, Others) can gain access to the system if approved by Management. Access controls are in place and are enforced primarily by controlling access to the Windows based operating system and by controlling access to AFTRAK itself through the use of user roles that grant permissions to create, update, and delete data within a specified organization data scope for those permissions. These roles and the organizational scope rights are defined within the CIMIS user management functions.

For a complete listing of user roles and their permissions, please see the Permissions Modules in DOORS. This matrix is too large to include in this document, but can be obtained by contacting the “Requesting Contact” named at the beginning of this document.

Any contractor users of the system have an approved moderate background investigation completed by National Background Investigation Center (NBIC).

9. How is access to the data by a user determined and by whom?

CIMIS

Access is granted on a need-to-know basis by CI management, and is restricted through the use of user roles identified in the CIMIS application. Access is documented through the use of logs and audit trails.

- Every user obtaining access to CIMIS is assigned a user role that determines his access to data. The user’s scope/level of access is based on a need to know, as determined by management. For example, agents may view their own employee data (personnel and time reporting) as well as investigative data pertaining to their assignments (investigative). Management has access to their own data and employees they supervise (personnel) as well as all investigations they have supervisory authority over (investigations). Support personnel (all areas), administrators (data base administration) and developers (upgrades, repairs, troubleshooting) are governed by the same rules.

- The CI employee requesting permissions in the CIMIS system, hereinafter referred to as the “user”, must first have an active, valid CI network account. In order for the user to have been granted a CI network account, the user must meet rigorous requirements which include mandatory drug testing and background investigation. Contractors receive restricted access based also on their need to know as determined by CI management and must pass a drug test and limited background check.

- Each office is advised to have a primary and backup person serving as the local office CIMIS User Administrator. User roles are determined by management based on five broad subject areas within the system: personnel, equipment, investigation, time reporting, and administration. Based on the user’s responsibility, the administrator will provide the user with the user information that must be entered in the Online 5081 (OL5081) system when requesting new or modified access.

- The OL5081 process is used to document access requests, modifications, and terminations for all types of users. A user’s manager or designated official must approve the addition of, modification of, or deletion of, the user’s role(s) and organizational data scope.

- The approved request is then electronically forwarded to the local office user administrators, who will review and approve the request for permissions as the FSC/USR in OL5081. These CIMIS subject matter experts (SMEs) have been specifically trained in proper user administration.

- Lastly, the approved request is then electronically forwarded to the HQ persons designated to provide the final approval as the Security/SA official. Subsequently, the requesting user is notified by the OL5081 system that the request has been granted.

- Once the request has been approved by the FSC/USR, the actual creating or editing of user profiles in CIMIS may be done by either the local office User Administrator or the HQ CIMIS user administrators.

AFTRAK

The AFTRAK Program Manager reviews and approves Online 5081 requests for access to the system. Users are assigned to those roles (with associated permissions) that support the tasks they need to perform to complete their job duties.

- Every user obtaining access to AFTRAK is assigned a user role that determines his/her access to data. The user’s scope/level of access is based on a need to know, as determined by management.

- The CI employee requesting permissions in the AFTRAK system, hereinafter referred to as the “user”, must first have an active, valid CI network account. In order for the user to have been granted a CI network account, the user must meet rigorous requirements which include mandatory drug testing and background investigation. Contractors receive restricted access based also on their need to know as determined by CI management and must pass a drug test and limited background check.

- The OL5081 process is used to document access requests, modifications, and terminations for all types of users. A user’s manager or designated official must approve the addition of, modification of, or deletion of, the user’s role(s) and organizational data scope.

- After the request has been approved, it is electronically forwarded to the appropriate individuals who can grant the user access to AFTRAK.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.

CIMIS

Yes. CIMIS does not receive any data from other IRS systems; however, the following systems receive limited data from CIMIS:

- Legacy AFTRAK
- ISDM

- PIOneer
- ITAMS
- AFTRAK
- IDA

The list of data elements received by each system is too extensive to include in this document. Please reference the CIMIS Interface Control Document for more information. This document can be obtained by contacting the “Requesting Contact” named at the beginning of this document.

AFTRAK

Yes. CIMIS is directly integrated with the AFTRAK application. CIMIS provides AFTRAK with investigation and warrant information for which CIMIS is the system of record.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

CIMIS

- Legacy AFTRAK
  - C&A – 6/19/2009
  - PIA – 3/12/2009

- ISDM
  - C&A – 1/27/2009
  - PIA – 7/08

- PIOneer
  - C&A – 2/4/2009
  - PIA – 2/4/2009

- ITAMS
  - C&A – 6/5/06
  - PIA – 4/28/06

- AFTRAK[1]
  - C&A – Tentatively scheduled ST&E 2/2010
  - PIA – Tentatively scheduled 8/2009

- IDA[2]

[1] CIMIS will provide Live Data to AFTRAK after the Security Certification, Privacy Impact Assessment, and Live Data Request Request have been approved.

[2] CIMIS will follow the guidelines outlined in IRM 10.8.8 as it pertains to Live Data. For systems/environments that do not have an approved Security Certification and Privacy Impact Assessment, CIMIS will only provide Live Data upon receipt of an approved Live Data Request form.

- C&A – Under development
    - PIA – Under development

AFTRAK

- CIMIS
    - C&A – 2/25/2009
    - PIA – 10/22/2008

12. Will other agencies provide, receive, or share data in any form with this system?

CIMIS

Yes. CIMIS does not receive any data from other agencies; however, CIMIS may provide the following information:

- Audit logon information to the GAO and/or TIGTA pursuant to an investigation and/or their oversight function.
- Investigation information to the DOJ, FinCEN, TIGTA, and TECS.
- Equipment information to the Department of Treasury, GSA, and the GAO.
- A data extract to the FinCEN, the administrator of the Bank Secrecy Act (BSA).

AFTRAK

Yes. The TEOAF receives Title 18, 21, and 31 monthly and quarterly paper reports, and various ad hoc reports from AFTRAK via manual transmission. A formal data sharing agreement exists with TEOAF. AFTRAK will receive an extract from the DOJ containing information pertaining to the state of the RASR.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

CIMIS

Data is never eliminated. Per IRM 1.15.30.1, "The records described in Item 15, Investigative files, are frozen; therefore, disposal is not authorized at this time." Per IRM Exhibit 1.15.30-1, investigative files are described as follows:

Investigative Files. Prosecution, non-prosecution and discontinued investigations (including withdrawal reports) together with related exhibits, workpapers, forms, correspondence and relative data that pertains to actual or alleged income and other tax evasions, wagering, coin-operated gaming devices, occupational and excise taxes, electronic surveillance recordings, memorandum, notes, etc., whether conducted by the IRS or received by the IRS from other sources, and other Actions investigated by the Criminal Investigation Division independently or jointly with other components of the Service.

- (1) Regional office.
  - (a) Disposal not authorized.
- (2) District offices.
  - (a) Disposal not authorized.
  - (b) Retire to Federal Records Center 2 years after case is closed.

(Note: If the Chief sees an impending need for the case file to effect civil settlement, or if the case is of significant interest, the file may be retained and returned to the Federal Records Center when no longer needed.)

AFTRAK
Records are maintained, administered and disposed of in accordance with IRM 1.15.30 Records Management, Records Control Schedule for Criminal Investigation, January 1, 2003. The IRM allows that investigative files are frozen and, therefore, disposal is not authorized at this time.

14. Will this system use technology in a new way?

CIMIS
No. CIMIS will not use technology in a new way.

AFTRAK
No. This system will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.

CIMIS
Yes. CIMIS is the vehicle that collects, compiles, and delivers information on investigative activities to target an individual or group for tax law violations.

AFTRAK
No. AFTRAK will not used to identify or locate individuals or groups.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.

CIMIS
Yes. Monitoring the case lifecycle against an individual, organization, business, etc is the business purpose of the system.

AFTRAK
No. AFTRAK will not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.

CIMIS
Yes. CIMIS is the vehicle that collects, compiles, and delivers information on investigative

activities to target an individual or group for tax law violations. Therefore, by creating a case against a person who violates tax laws, CIMIS treats him/her differently from those who do not.

AFTRAK

No. Use of AFTRAK will not allow IRS to treat taxpayers, employees, or others differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

CIMIS

Yes. CIMIS stores information on criminal investigations which are placed in our judicial system which adheres strictly to the concept of due process.

AFTRAK

No. AFTRAK is only an inventory tool and does not have the capability to make negative determinations.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

CIMIS

CIMIS is an intranet web-based system for authorized CI employees. Cookies are not used to track access. Audit logs and trails are used by CIMIS to track CI user access.

AFTRAK

AFTRAK is an intranet web-based system for authorized CI employees. Cookies are not used to track access. Audit logs and trails are used by AFTRAK to track CI user access.

View other PIAs on IRS.gov